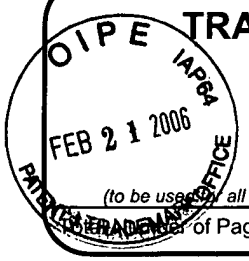
PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

ZPW
AF



TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 23

Application Number	10/737,389
Filing Date	December 16, 2003
First Named Inventor	En-Yi Liao
Art Unit	2141
Examiner Name	Serrao, Ranodhi N
Attorney Docket Number	10033.000400

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form
- ☒ Fee Attached
- ☐ Amendment / Reply
- ☐ After Final
- ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
- ☐ Reply to Missing Parts under 37 CFR1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below)*:
  Return Receipt Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm	Okamoto & Benedicto LLP		
Signature	Patrick Benedicto		
Printed Name	Patrick D. Benedicto		
Date	February 16, 2006	Reg. No.	40,909

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	Patrick Benedicto		
Typed or printed name	Patrick D. Benedicto	Date	February 16, 2006

Docket No. 10033.000400
Appeal Brief
February 16, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

En-Yi Liao

Application No.: 10/737,389 Examiner: Serrao, Ranodhi N.

Filing Date: December 16, 2003 Art Unit: 2141

Assignee: Trend Micro Incorporated

Title: Technique For Intercepting Data In A Peer To Peer Network

---

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF FILED UNDER 37 C.F.R. § 41.37

Sir:

This appeal brief follows the Notice of Appeal filed by Applicants on February 15, 2006.

A check covering the fee for filing an appeal brief is submitted herewith. If for any reason the check is insufficient or additional fees are required, the Commissioner is hereby authorized to charge the insufficiency to Deposit Account No. 50-2427.

I. REAL PARTY IN INTEREST

The real party in interest is Trend Micro Incorporated, which is the assignee of the present application.

02/21/2006 CCHAU1 00000025 10737389
01 FC:1402 500.00 OP

II. RELATED APPEALS AND INTERFERENCES

On information and belief, there are no appeals, interferences, or judicial proceedings known to the appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board of Patent Appeals and Interferences (the "Board") decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-22 are pending in this application and stand finally rejected.

Claims 1-22 are being appealed. These claims are rejected in the final office action mailed December 23, 2005 ("last office action").

IV. STATUS OF AMENDMENTS

No amendment has been filed after the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter relates to interception of data in a peer to peer network. In a conventional peer-to-peer network, data transfer between two peer computers ("peer nodes") are performed directly between the computers. This direct data transfer may result in the spread of computer viruses, for example. To address problems relating to peer-to-peer data transfers, embodiments of the invention allow for redirection of data from a sender peer node to an interception node, where the data can be processed (e.g., scanned for viruses) prior to forwarding the data to the destination peer node.

Independent claim 1 recites a method of transferring data in a peer-to-peer computer network that includes a first peer node and a second peer node (see Specification, FIG. 3, data transfer between peer nodes 110-1 and 110-2 through interception node 330). The method provides the second peer node the location information of an interception node instead of the location information of the first peer

node (Specification, page 11, lines 3-14). A communication channel is established between the second node and the interception node (Specification page 11, lines 14-16). The data being transferred in the peer-to-peer computer network (from preamble) is received in the interception node, where the data are processed (Specification page 12, lines 7-15).

Independent claim 10 recites a method of transferring a file in a peer-to-peer computer network (see Specification, FIG. 3, file transfer between peer nodes 110-1 and 110-2 through interception node 330). A file originally intended to be transferred directly (Specification, page 11, lines 3-5; page 15, lines 10-17) from the first peer node to the second peer node is redirected from a first peer node to an interception node (Specification, page 11, lines 12-19; page 12, lines 7-11), where it is processed (Specification, page 12, lines 11-12) prior to being transferred to the second peer node (Specification, page 12, lines 12-13).

Independent claim 16 recites a system for transferring data in a peer-to-peer network (see Specification, FIG. 3, data transfer between peer nodes 110-1 and 110-2 through interception node 330). A presence modifier detects the publication of location information of a first peer node (Specification, page 11, lines 5-8) and provides the second peer node the location information of the interception node instead of that of the first peer node (Specification, page 11, lines 12-14).

Independent claim 22 recites a method of transferring a file in a peer-to-peer computer network (see Specification, FIG. 3, data transfer between peer nodes 110-1 and 110-2 through interception node 330). A file originally intended to be transferred directly (Specification, page 11, lines 3-5; page 15, lines 10-17) from a first peer node to a second peer node is first transferred to an interception node Specification, page 11, lines 12-19; page 12, lines 7-11), where the file is scanned for viruses (Specification, page 10, lines 16-19; page 12, lines 11-12) prior to being transferred to the second node (Specification, page 12, lines 12-13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following are to be reviewed on appeal:

1. The rejection of claims 1-5, 7-11, 13, and 14 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,061,796 to Chen et al. ("Chen").

2. The rejection of claims 16 and 19 under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0028585 by Yeager et al. ("Yeager").

3. The rejection of claims 6 and 12 under 35 U.S.C. § 103(a) as being unpatentable over Chen in view of U.S. Patent No. 6,789,117 to Joiner et al. ("Joiner").

4. The rejection of claim 15 under 35 U.S.C. § 103(a) as being unpatentable over Chen in view of Yeager.

5. The rejection of claims 17, 18, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Yeager in view of Joiner.

6. The rejection of claim 21 under 35 U.S.C. § 103(a) as being unpatentable over Yeager in view of Chen.

7. The rejection of claim 22 under 35 U.S.C. § 103(a) as being unpatentable over Chen and Joiner.

VII. ARGUMENTS

Applicants traverse the rejection of claims 1-22 for the following reasons.

A. CLAIMS 1-5, 8, and 9

Claims 1-5, 8, and 9 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,061,796 to Chen et al. ("Chen").

To anticipate a claim, a reference must include all the limitations of the claim.

Claim 1 is patentable over Chen at least for reciting: "in a data transfer between the first peer node and the second peer node" and "receiving the data in the interception node." That is, claim 1 requires the data to be transferred between two peer nodes to be received in the interception node. In Chen, the authentication server provides authentication services and is thus passed authentication information by the shim 50. However, data to be transferred between peer computers do not pass through the

authentication server ("interception node") or any node on the network whose location information has been substituted for that of the destination computer (Chen, FIG. 6, channel 62; col. 11, line 59 to col. 12, line 19). For example, Chen is explicit that:

> "...the peer-to-peer applications are designed only to communicate with "peers" 45 and **not with the authentication server**..."

Chen, col. 9, lines 62-64 (emphasis added)

In other words, in Chen, data to be transferred between two peer nodes are directly transferred between the peer nodes.

Chen is also explicit that it provides for interception of **function calls** (Chen col. 11, lines 24-29), not the data to be transferred between peer nodes. This creates a serious problem as direct data transfer between peer nodes may result in proliferation of computer viruses (e.g. see Specification, page 3, lines 3-9).

> "In the case of a **peer-to-peer application**, in which the clients wish to communicate over a direct link 62, the invention provides for the **function calls** establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23."

Chen col. 11, lines 24-29 (emphasis added)

Chen col. 11, lines 24-49, cited in the rejection of claim 15, explains the role of the authentication server in a peer-to-peer communication. In the case where clients communicate **over a direct link 62** (see Chen, FIG. 6), the authentication server opens a secured channel 63 to an authentication client software to perform an authentication procedure and transmit **session keys** for decrypting communications sent over the channel 62 (the direct link where data transfer is performed). Note that only authentication communications pass through the authentication server; in peer-to-peer communications, data transfer is over a direct channel 62.

Claim 1 is further patentable over Chen at least for reciting: "**providing** the second peer node a location information of an interception node **instead** of a location information of the first peer node in a data transfer between the first peer node and the second peer node" (emphasis added). Chen discloses a virtual private network with centralized authentication services for peer nodes. In Chen, the socket shim 50 is used to

intercept function calls (Chen, col. 9, lines 42-59) to allow for authentication by an authentication server. Chen is explicit that:

> "Since the basic authentication client software is designed to send all communications directly to the authentication server, while the peer-to-peer applications are designed only to communicate with 'peers' 45 and not with the authentication server, **the principal function of shim 50 is to arrange for the destination of address of the communication to be supplied to both the authentication client software and to authentication server**, even though the peer application assumes that it is communicating only with the peer application."
>
> Chen, col. 9, line 60 to col. 10, line 2 (emphasis added)

That is, in Chen, the sender computer is not provided the location information of the authentication server (or another server) instead of that of the receiving computer. In contrast, claim 1 requires the second node to be provided the location information of the interception node. In fact, in Chen, **the sender computer must send the authentication server computer the address of the receiving computer**. This point is reiterated in Chen's Abstract:

> "Where the parties to the communication are peer-to-peer applications, the intercepted function calls, requests for service, or data packets include **the destination address of the peer application, which is supplied to the server** so that the server can authenticate the peer and enable the peer to decrypt further direct peer-to-peer communications."
>
> Chen, Abstract (emphasis added)

This is **opposite** to what is recited in claim 1, where the second peer node is expecting to be provided the location information of the first peer node but is instead provided the location information of the interception node.

Further note that claim 1 specifically recites "location information of an interception node **instead** of a location information of the first peer node." That is, to intercept the data, one location information is substituted for another. This does not happen in conventional packet exchanges as the destination and source addresses therein are the ones supposed to be in the packet in the first place.

For at least the above reasons, it is respectfully submitted that claim 1 is patentable over Chen.

Claims 2-5, 8, and 9 depend on claim 1, and are thus patentable over Chen at least for the same reasons claim 1 is patentable.

B. CLAIM 7

Claim 7 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Chen.

Claim 7 recites that the contents of the data are filtered **in the interception node**. Chen, col. 9, lines 42-59, cited in the rejection of claim 7, discusses the functionality of the shim 50, which is in a client (Chen, FIG. 3) and **not in the authentication server** ("interception node"). Chen does not disclose or suggest filtering the contents of data to be transferred between two peer nodes in the authentication server. As explained above, filtering of data in the authentication server is suspect given that data transfer does not even go through the authentication server in the first place. Filtering of data in Chen's authentication server is further suspect given that data being transferred is **encrypted** and can only be decrypted in a peer node. In Chen, the encryption and decryption are performed in the sending and destination computers (Chen, FIG. 7, steps 106 and 109; col. 12, lines 11-26; Abstract), not in the authentication server. The authentication server merely provides session keys to peer nodes.

Therefore, it is respectfully submitted that claim 7 is patentable over Chen.

C. CLAIMS 10 and 11

Claims 10 and 11 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Chen.

Claim 10 is patentable over Chen at least for reciting: "redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node." As explained above in regard to claim 1, files to be transferred between peer nodes are NOT redirected in Chen. In Chen, file transfer can only occur between peer-to-peer applications in peer nodes (Chen, col. 9, lines 62-64, col. 10 lines 2-4; FIG. 6, channel 62).

Chen col. 6, line 66 to col. 7 line15, cited in the last office action, discusses the functionality of the shim 50, which intercepts **function calls** to redirect **initial**

communications to establish a secured communication. Nothing in that cited section discloses or suggests redirecting to the authentication server files to be transferred between two peer nodes. On the contrary, as explained above, peer nodes perform direct data transfer in Chen.

Chen col. 9, lines 42-49, cited in the last office action as disclosing "processing the file in the interception node" discusses the functionality of the shim 50, which is in a client (Chen, FIG. 3) and **not in the authentication server** ("interception node").

Chen col. 10, lines 37-58, cited in the last office action as disclosing "transferring the file from the interception node to the second peer node" discusses the operation of the driver shim 55 in a client computer, but contains no disclosure as to file transfers to from the client computer to the authentication server. As explained in the discussion of claim 1 above, file transfer in Chen is directly between peers (as is conventional) and does not pass through the authentication server.

For at least the above reasons, it is respectfully submitted that claim 10 is patentable over Chen.

Claim 11 depends on claim 10, and is thus patentable over Chen at least for the same reasons claim 10 is patentable.

D. CLAIM 13

Claim 13 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Chen.

Claim 13 recites that the **content of the file** is filtered **in the interception node**. Chen, col. 9, lines 42-59, cited in the rejection of claim 13, discusses the functionality of the shim 50, which is NOT in the authentication server ("interception node") in the first place. Chen does not disclose or suggest **filtering** the content of a file in the authentication server. In Chen, files to be transferred between two peer nodes do not even pass through the authentication server. Filtering of files in Chen's authentication server is also suspect given that files transferred between peer nodes are encrypted.

Therefore, it is respectfully submitted that claim 13 is patentable over Chen.

E. CLAIM 14

Claim 14 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Chen.

Claim 14 recites: "informing the second peer node that an address of the first peer node is that of the interception node." In the rejection of claim 14, the last office action suggests that Chen, in col. 12, lines 11-32, discloses the aforementioned limitation. This conclusion is respectfully traversed in that Chen, as explained above, relies on a shim to perform interception of authentication information, not files being transferred between two peer nodes. The cited section of Chen describes the method of FIG. 7, which involves the client program 20 receiving the destination peer address, which is eventually provided to the authentication server upon interception by the shim. However, the sending computer is **not informed that the address of the receiving computer is that of the authentication server**, as required by claim 14. In Chen, the sending computer needs a shim that provides the location information of the destination computer to the authentication server instead of the other way around.

Therefore, it is respectfully submitted that claim 14 is patentable over Chen.

F. CLAIMS 16, 19, and 21

Claims 16 and 19 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0028585 by Yeager et al. ("Yeager").

Claim 16 is patentable over Yeager at least for reciting: "the presence modifier being configured to provide to a second peer node a location information of an interception node **instead of** the location information of the first peer node **in response to** a detection of the publication" (emphasis added). Yeager pertains to trust mechanisms in peer-to-peer networks. However, Yeager does not teach or suggest a presence modifier providing a peer node location information of an interception node instead of the location information of another peer node in response to detection of the publication of the location information of the peer node.

Yeager paragraphs [0013], [0162], and [0173] are cited in the rejection of claim 16. Yeager paragraph [0013] discusses peer-to-peer networks in general. Yeager paragraph [0162] introduces the concept of peer-to-peer authorization services and publication of addresses for authorization peers. Yeager paragraph [0173] discloses that

a certificate on a key ring may include a peer identifier, the address of the certificate's subject or owner, and the local peer's certificate confidence for that certificate. None of the cited paragraphs discloses or suggests providing a second peer node the location information of an interception node **instead of that of a first peer node** in response to detection of the publication of the location information of the first peer node. The Yeager trust mechanisms have nothing to do with substituting an address of an interception node for that of a peer node, let alone doing so in response to a publication of the location information of another peer node.

Therefore, it is respectfully submitted that claim 16 is patentable over Yeager.

Claim 19 depends on claim 16 and is thus patentable over Yeager at least for the same reasons that claim 16 is patentable.

Claim 21 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Yeager as applied to claim 16 and further in view of Chen.

The patentability of claim 16 over Yeager has already been explained above. Chen does not add anything to Yeager in regard to claim 16. Claim 21 depends on claim 16 and is thus patentable over Yeager and Chen at least for the same reasons that claim 16 is patentable.

G. CLAIMS 6 and 12

Claims 6 and 12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Chen in view of U.S. Patent No. 6,789,117 to Joiner et al. ("Joiner").

There are three requirements to establish a prima facie case of obviousness. First, there must be some suggestion or motivation to modify a reference or to combine references. Second, there must be a reasonable expectation of success. Third, the prior art reference or combined references must teach or suggest all the claim limitations. See MPEP § 2143.

Claim 6 is patentable over Chen and Joiner at least for reciting: "wherein processing the data in the interception node comprises scanning the data for computer viruses." As noted in the last office action, Chen does not disclose scanning data for

computer viruses in the interception node. However, the last office action suggests that it would have been obvious to use the teachings of Joiner to perform virus scanning in Chen's authentication server ("interception node").

Joiner pertains to network analysis using an agent/host controller interface. Joiner col. 13, line 65 to col. 14, line 4, cited in the last office action, discusses scanning of network traffic for computer viruses in the host controllers 1002 (Joiner, col. 13, lines 54-64). Note, however, that host controllers 1002 are designed to cooperatively work with agents 900, not between peer nodes. That is, host controllers 1002 do not scan data being transferred between peer nodes in a peer-to-peer network. This is not surprising given that conventional data transfer between peer nodes are not scanned for viruses in transit, but rather in the peer nodes themselves. This is a type of problem specifically being addressed by claim 6 (e.g. see Specification, page 3, lines 3-6). Virus scanning of data in transit between two peer nodes is taught only in the present disclosure, not in any of the references of record. Therefore, there is simply no suggestion or motivation to modify Chen or to combine Chen and Joiner to scan peer-to-peer data for computer viruses in an interception node, without using the present application as a blue print. Joiner itself does not perform virus scanning of data in transit.

Another problem with the Chen and Joiner combination is that data in Chen's authentication server are **encrypted**. In Chen, the encryption and decryption are performed in the sending and destination computers (Chen, FIG. 7, steps 106 and 109; col. 12, lines 11-26). Neither Chen nor Joiner discloses or suggests how virus scanning can be performed on encrypted data in a server between two peer nodes that perform local encryption and decryption. Therefore, data transferred between two peer nodes in Chen can only be scanned for viruses in either the sending or destination peer node, not in a host controller or authentication server. Because virus scanning cannot be performed on Chen's encrypted in-transit data, the combination of Chen and Joiner has no reasonable expectation of success.

Yet another problem with the Chen and Joiner combination is that in Chen, data to be transferred between two peer nodes do not pass through an intermediate server (see discussion with regard to claims 1 and 10 above). That is, in Chen, data are transferred

directly between two peer nodes. There is no "interception node" where virus scanning can be performed in the first place. This is especially problematic as it requires both peer nodes to have antivirus software. Therefore, the combination of Chen and Joiner does not and cannot teach all the limitations of claim 6, and has no reasonable expectation of success.

Claim 12 is similarly patentable over Chen and Joiner.

For at least the above reasons, it is respectfully submitted that claims 6 and 12 are patentable over Chen and Joiner.

H. CLAIM 15

Claim 15 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chen as applied to claim 10 and further in view of Yeager.

Claim 15 depends on claim 10. The patentability of claim 10 over Chen has already been explained above. As previously explained, Chen does not disclose or suggest file transfer between two peer nodes passing through an interception node. This is not surprising considering conventional peer-to-peer communication is primarily directly between two peer nodes. Yeager does not add anything to Chen in regard to claim 10.

The last office action suggests it would have been obvious to combine the teachings of Chen and Yeager to allow for "querying a P2P server for location information of peer nodes involved in a transfer of the file; based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node," as recited in claim 15. This combination is suspect for several reasons. Firstly, the peer nodes in Chen include a shim for redirecting authentication information to the authentication server including the address of a destination peer node. Chen's VPN network does not need a P2P server for identifying nodes involved in a file transfer because such information is already provided by the shim to the authentication server in order to establish communication between peer-to-peer clients involved in the file transfer. A P2P server with location information of nodes involved in file transfer

would thus be redundant in Chen's VPN network. Therefore, there is no suggestion or motivation to modify Chen's VPN network to make use of a P2P server.

Secondly, peer nodes in Chen will not be able to communicate with such a P2P server because communication between the peer nodes is encrypted and requires authentication services from the authentication server. Therefore, the combination of Chen and Yeager has no reasonable expectation of success.

Thirdly, Chen's peer nodes have no need for Yeager's trust mechanism because Chen's authentication server, the gist of Chen's invention, already authenticates the peer nodes. Again, there is no suggestion or motivation to modify Chen with the teachings of Yeager.

I. CLAIMS 17, 18, and 20

Claims 17, 18, and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yeager as applied to claim 16 and further in view of Joiner.

Claim 17 recites a data scanner configured to scan data passing through the interception node of claim 16. As noted in the last office action, Yeager does not disclose a data scanner configured to scan data passing through the interception node. Yeager does not have an interception node on which to do data scanning. This is not surprising as Yeager's trust mechanism is for peer-to-peer communication, and conventional peer-to-peer communication is directly between peers.

The last office action suggests, however, that it would have been obvious to use Joiner's "interception node" to scan data transferred between two peer nodes in Yeager's peer-to-peer network. There are several problems with this conclusion. Firstly, conventional peer-to-peer data transfer does not involve an interception node between two peer nodes. Joiner's host controller ("interception node") does not stand between two peer nodes involved in peer-to-peer data transfer. Neither Joiner nor Yeager discloses or suggests that data being transferred between two peer nodes should be scanned in an interception node. Such a teaching is only taught in the present disclosure, **NOT** in Joiner or Yeager. Therefore, one of ordinary skill in the art would not be

motivated to modify Yeager's peer-to-peer network to include Joiner's "interception node," and such combination cannot teach or suggest all the limitations of claim 17.

Secondly, neither Yeager nor Joiner teaches or suggests ***how*** data in a peer-to-peer communication (which conventionally is a direct communication between two peer nodes) can be redirected through Joiner's host controller. The teaching on how to do so is in the present disclosure, not in Yeager or Joiner. Therefore, the combination of Joiner and Yeager has no reasonable expectation of success, and cannot teach or suggest all the limitations of claim 17.

Claim 18 recites that the interception node of claim 1 is separate from a P2P server. As explained above in regard to claim 17, one of ordinary skill in the art would not be motivated to modify Yeager's peer-to-peer network to include Joiner's "interception node."

Claim 20 recites that the data scanner of claim 17 is configured to scan the data for computer viruses. The patentability of claim 17 over Yeager and Joiner has already been explained. Conventional peer-to-peer data transfer does not involve an intermediary server, and thus do not involve virus scanning other than in the peers involved in the data transfer. Furthermore, there is no teaching on how Joiner's "interception node" can be placed in the data transfer path of Yeager's peer nodes involved in peer-to-peer communication.

J. CLAIM 22

Claim 22 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chen and Joiner.

Claim 22 is patentable over Chen and Joiner at least for reciting: "transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node" and "scanning the file for viruses in the interception node. As previously explained, there are at least three problems with this combination. Firstly, in Chen, file transfer between two peer nodes do pass through an interception node. There is no interception node where the file can be

scanned for viruses. Joiner's interception node is not and cannot be placed between two of Chen's peer nodes. Secondly, files transferred between two of Chen's peers are encrypted and can only be decrypted in one of the peers. Thirdly, neither Chen nor Joiner discloses or suggests virus scanning of files in-transit between peer nodes. It is respectfully submitted that such virus scanning is not performed in the prior art (e.g. Chen, Joiner, and Yeager) because peer-to-peer file transfer is, by default, directly between peers. This is the main reason why peer-to-peer networks are established in the first place. Claim 22 breaks this convention to allow for virus scanning in a peer-to-peer file transfer without substantially impacting the use of such peer-to-peer networks.

For at least the above reasons, it is respectfully submitted that claim 22 is patentable over Chen and Joiner.

VIII. CLAIMS INVOLVED IN THE APPEAL

The claims involved in the appeal are included in the Appendix submitted herewith.

IX. CONCLUSION

For at least the above reasons, allowance of claims 1-22 is respectfully requested.

Respectfully submitted,
En-Yi Liao

Dated: 2/16/2006

Patrick Benedicto

Patrick D. Benedicto, Reg. No. 40,909
Okamoto & Benedicto LLP
P.O. Box 641330
San Jose, CA 95164
Tel.: (408)436-2110
Fax.: (408)436-2114

CERTIFICATE OF MAILING			
I hereby certify that this correspondence, including the enclosures identified herein, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.			
Signature:	Patricia Benedicto		
Typed or Printed Name:	Patrick D. Benedicto	Dated:	February 16, 2006
Express Mail Mailing Number (*optional*):			

CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL

1. A method of transferring data in a peer-to-peer computer network that includes a first peer node and a second peer node, the method comprising:

providing the second peer node a location information of an interception node instead of a location information of the first peer node in a data transfer between the first peer node and the second peer node;

establishing a communication channel between the interception node and the second peer node;

receiving the data in the interception node; and

processing the data in the interception node.

2. The method of claim 1 wherein the data are received by the interception node from the second peer node.

3. The method of claim 1 further comprising:

establishing a communication channel between the interception node and the first peer node; and

wherein the data are received by the interception node from the first peer node.

4. The method of claim 1 wherein the data comprise a file.

5. The method of claim 1 wherein the location information of the first peer node comprises an IP address and a port number.

6. The method of claim 1 wherein processing the data in the interception node comprises scanning the data for computer viruses.

7. The method of claim 1 wherein processing the data in the interception node comprises filtering the content of the data.

8. The method of claim 1 further comprising:

transferring the data from the interception node to the second peer node after the data have been processed in the interception node.

9. The method of claim 1 further comprising:

transferring the data from the interception node to the first peer node after the data have been processed in the interception node.

10. A method of transferring a file in a peer-to-peer computer network, the method comprising:

redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

processing the file in the interception node; and

transferring the file from the interception node to the second peer node.

11. The method of claim 10 wherein the peer-to-peer computer network includes the Internet.

12. The method of claim 10 wherein processing the file in the interception node comprises scanning the file for viruses.

13. The method of claim 10 wherein processing the file in the interception node comprises filtering a content of the file.

14. The method of claim 10 wherein redirecting the file comprises:

informing the second peer node that an address of the first peer node is that of the interception node.

15. The method of claim 10 wherein transferring the file from the interception node to the second peer node comprises:

querying a P2P server for location information of peer nodes involved in a transfer of the file;

based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node; and

transferring the file from the interception node to the second peer node.

16. A system for transferring data in a peer-to-peer network, the system comprising:

a presence modifier configured to detect a publication of a location information of a first peer node, the presence modifier being configured to provide to a second peer node a location information of an interception node instead of the location information of the first peer node in response to a detection of the publication, the first peer node and the second peer node being computers in the peer-to-peer computer network.

17. The system of claim 16 further comprising:

a data scanner in the interception node, the data scanner being configured to scan data passing through the interception node.

18. The system of claim 16 wherein the interception node comprises a computer that is separate from a P2P server.

19. The system of claim 16 wherein the location information of the first peer node comprises an IP address and a port number.

20. The system of claim 17 wherein the data scanner is configured to scan the data for computer viruses.

21. The system of claim 16 further comprising:

a transfer manager in the interception node, the transfer manager being configured to obtain session information from the presence modifier.

22. A method of transferring a file in a peer-to-peer computer network, the method comprising:

transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

scanning the file for viruses in the interception node; and

transferring the file from the interception node to the second peer node.

EVIDENCE APPENDIX

There are no documents or items submitted under this section.

RELATED PROCEEDINGS APPENDIX

There are no documents or items submitted under this section.